AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

9923 Stone Wood Court
Burke, VA, 22015

Case No. 1:19-sw-1415

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A and 2422	Distribution, Receipt and Possession of Child Pornography; and Online Enticement

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

AUSA Jessica D. Aber

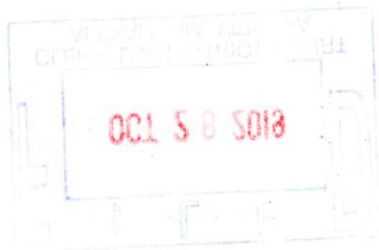
Special DUSM John Houlberg, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/28/2019

City and state: Alexandria, Virginia

/s/
Ivan D. Davis
United States Magistrate Judge


OCT 28 2019

ATTACHMENT A

Property to be searched

The property to be searched is 9923 Stone Wood Court, Burke, VA, 22015, further described as a split-level style single dwelling house. The house consists of a combination of brick and gray vinyl siding, with black shutters. There is a concrete driveway is at the right edge of the property which leads to an attached garage with a single garage door. Above the garage in black script are the letters written out "Ninety-Nine Twenty-Three". There is a sidewalk leading from the driveway to the front door of the residence, which is situated approximately in the center of the front of the residence. The front door appears to be a solid 4 panel door with a small glass window on the top of it, and has a glass storm door attached to it. On the left side of the residence is another entry door. This door appears to be a white door with glass windows on the top half of it.

ATTACHMENT B

Property to be seized

1. All records and information relating to possible violations of the following criminal offenses: distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252A; and online enticement, in violation of 18 U.S.C. § 2422(b), including:

   a. Any and all visual depictions of minors;

   b. Any and all communications with minors;

   c. Any and all address books, names, and lists of names and addresses of minors;

   d. Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;

   e. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;

   f. Records and information relating to Alt.com and/or Kik username/account jmsoqueenIVY, Joe Smo, Carika2016, and any related Alt.com or Kik accounts;

   g. Records and information relating to the email accounts "joesmo@coxnet" and any related email accounts;

   h. Any information recording suspect's schedule or travel from October 23, 2019 to October 24, 2019.

2. Computers or storage media (hereinafter, "COMPUTER") used as a means to commit the violations described above.

3. For any COMPUTER whose seizure is otherwise authorized by this warrant, and any COMPUTER that contains or in which is stored records or information that is otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect the COMPUTERS to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smart phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

* * *

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF:
9923 Stone Wood Court
Burke, VA 22015

Case No. 1:19-sw-1415

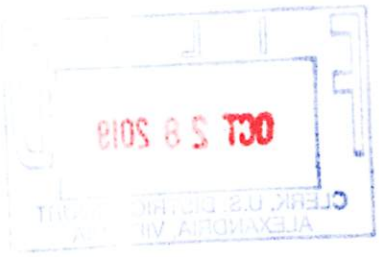
AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, John Houlberg, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 9923 Stone Wood Court, Burke, VA, 22015, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Virginia State Police Bureau of Criminal Investigation, General Investigations Section, and have been since 1999. I am currently assigned as a Task Force Officer (TFO) to the Federal Bureau of Investigation, Richmond Division Child Exploitation Task Force and have been since 2011. I have been deputized as a Special Deputy United States Marshal since May 20, 2011. I am thus an officer of the United States who is empowered by law to conduct investigations of, and make arrests for, offenses enumerated in Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422 involving child exploitation offenses.


OCT 28 2019
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

3. During my career in law enforcement, I have received extensive training in the conduct of a variety of investigations, including child exploitation. In the course of my employment as a sworn law-enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18 of the United States Code, including § 2252A, involving distribution, receipt, and possession of child pornography, and § 2422(b), involving online enticement or coercion of a minor to engage in illegal sexual activity.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

A. Communications with the OCE

5. The FBI Richmond Division's Child Exploitation Task Force located in Richmond, Virginia, conducted an ongoing undercover operation targeting subjects willing to travel in order to engage in sex with a minor. During the operation, online covert employees (OCEs) used covert social media accounts to pose as an adult intermediary who has access to female minors. The OCE's posted profiles on a number of online platforms and subsequently responded to subjects who indicated a desire to meet with the female minors.

6. An OCE posted one such undercover (UC) profile on "Alt.com." Alt.com is a network for members interested in alternative forms of sexual relationships and friendship. Users

can bond over fetishes, kinks, and BDSM (Bondage, Discipline, Sadism, and Masochism), as well as explore the site's large stockpile of sexual videos, articles, and other content. The OCE's Alt.Com profile displayed a picture of a female law enforcement officer (LEO) who is currently employed with the City of Richmond Police Department. The UC profile showed that the user was a middle-aged female from central Virginia. The profile also included a list of kinks to include "young/old," "infantilism/Diapers," "Bestiality," and "taboo family." Between April 17, 2018 and August 12, 2019, an individual, sent electronic messages to the UC profile seven times using the user name "jsmoqueenIVY".

7. On July 29, 2019, "jsmoqueenIVY" wrote, "I want to talk to you about Taboos. Preferably in person but let's start by messages including email if you want. My email is joesmo@coxnet. I have met others here and on kik and tumblr that have same interests".

8. On August 12, 2019, "jsmoqueenIVY" wrote, "Hi still would love to talk to you about your kinks. We may have things in common and would love to eventually meet to chat in person". On August 13, 2019, the OCE asked "jsmoqueenIVY" if he had KIK and he responded "Yes Joe Smo username Carika2016". The OCE provided an undercover KIK user name on August 23, 2019.

9. KIK is shorthand for Kik Messenger, a freeware instant messaging mobile app. It uses a smartphone's data plan or Wi-Fi to transmit and receive messages, photos, videos, or other content between user. KIK is known for features preserving users' anonymity, such as allowing user to register without providing a telephone number.

10. On Alt.com, "jsmoqueenIVY"'s profile displayed his picture and stated that the user was a 63 year-old male from Sterling, Virginia.

11. On August 25, 2019, "Joe Smo" subsequently contacted the OCE on KIK and stated "Hi Jenn or Jennifer. This is Louie from Alt" and sent a picture of himself. The OCE asked "Hi Joe..what's your name on alt again" and Joe Smo responded "Louie real name. Its long like Josm4queenivy?".

12. On August 27, 2019, the OCE advised her nieces were ages 6 and 10. Joe Smo responded "You have Lolita play with them? That's hot. I would love to watch that. I have a 13 and 15 year olds I've met on KIK that want to play. Neither one are virgins".

On August 30, 2019, the OCE and Joe Smo had the following exchange:

Joe Smo:	"Ever had 3somes".
OCE:	"sort of"
Joe Smo:	"Your nieces?"
OCE:	"yeah"
Joe Smo:	"That's hot" "It's actually amazing how many incestuous folks ive met on Tumblr and here in last 2 years. I thought I was a bit unique"
OCE:	"Yeah I'm finding there are a lot more that I thought of" "Thought I was unique too lol" "Glad you think it's hot"
Joe Smo:	"I do. Would love to watch"
OCE:	"Watch?"
Joe Smo:	"Well…unless invited to play too"
OCE:	"Oooh that would be fun"
Joe Smo:	"You're going to get me excited"
OCE:	"What would you like to do if you were invited to play? "Me too lol"
Joe Smo:	"Everything to be honest.." "I'd love to eat all of you"

"One on my face and one giving me head"
"Everyone busy lol"
OCE: "Omg that would be so hot"
Joe Smo: "Yes it would"

Joe Smo then sent a purported picture of himself on the bed in underwear with an erect penis.

13. The same day and shortly after the above exchange, Joe Smo sent a message to the OCE stating "Okay. I must admit I love young girls starting puberty", "Budding tits and fine pussy hair", and sent three images of young girls approximately 12 years old stating "Dude sent me these before". Two of the images are of juvenile females, approximately 10 years old with their shirts off exposing their breasts and one in a shirt with breasts poking through the shirt. Joe Smo then sent a picture of a female juvenile approximately 12 years of age, laying on a bed with her shirt pulled up exposing her breasts and her underwear pulled down exposing her vagina. The image exposing her vagina is taken from the knees up and the central focus of the image is her vagina. The child appears to be sleeping. Joe Smo states "I would so love to fuck her". The OCE responds "she looks older tho" and Joe Smo responds "12 or 13".

14. Joe Smo continues stating "I'm pretty thick but would be gentle and get you and 10 year old very wet first", "Love eating pussy".

15. On September 3, 2019, OCE tells Joe Smo "Fell asleep with Gracie last night...are you normally better to talk in the evenings?" Joe Smo responds "Yes. Gracie?". The OCE states "Oh sorry, my 6 yr old niece", "Krystal is the 10 yr old".

16. On September 10, 2019, OCE stated "I would most likely have the girls, that ok?" Joe Smo responded stating the following:

> "How old was your ex that played with 10 year old?"
> "Would her playing with me turn your on"
> "You two together would for me"

Joe Smo sent the OCE three images of underage girls, two in sexually suggestive poses and one sitting cross legged in a shirt and stated "All gorgeous girls".

OCE:	"I just meant its hard to find a babysitter but HELL YEAH!"
	"That'd be a lot of fun"
Joe Smo:	"I'd be so horny"
	"She may struggle on bjs...lol"
OCE:	"Lol why is that?"
Joe Smo:	"I'm thick"

17. On September 11, 2019, Joe Smo discussed a woman he chatted with who wanted him to take her 13-year-old daughter's virginity. Joe Smo then sent the OCE two images of what appear to be a 13-year old-girl. One image is of the juvenile standing towards a mirror taking a picture of her naked body. The second image is of the juvenile, in what appears to be a vehicle, pulling down her pants exposing her vagina. The primary focus of the image is the juvenile's vagina. OCE asks Joe Smo if the pictures are of her, and he responds yes. Joe Smo expressed disappointment in not being able to meet up with them and the OCE states "Oh well that's a shame!". Joe Smo responds with "Yes but now I've met you".

18. On September 17, 2019, Joe Smo provides the cell phone number 703-401-XXXX to the OCE for an additional means of communication.

19. On September 20, 2019, OCE and Joe Smo have the following exchange:

Joe Smo:	"Do the girls know about me? Expecially Kyrstal?"
OCE:	"Not yet, I didn't want to tell them until you were sure"
Joe Smo:	"Sure about?"
	"Playing?"
	"That's all ive been thinking about"
OCE:	"Yeah and visting etc"
	"Really?"

Joe Smo then sends the OCE two imges of two juveniles approximately 10 years old clothed in sexually suggestive poses, and one image of two juveniles naked and posing for the camera.

20. During the totality of the chats, Joe Smo mentioned visiting the OCE multiple times.

On October 20, 2019, the OCE had the following exchange with Joe Smo:

Joe Smo:	"Maybe I should visit"
OCE:	"Wish I could! Working today"
	"And if you want to visit we need to plan what's gonna happen"
	"You know, in case youre a serial killer"
	"I've only met up with one other guy, our regular and we had a plan beforehand."
Joe Smo:	"Sure, We can plan whatever you want. Easier to discuss on the phone but here's the basics: I visit and plan to spend the night. After I arrive we hug and chat a bit to feel more comfortable. We all go to dinner my treat. Ice cream after for the girls if they want. I know what you said you like but what does Khrys like? I want to kiss her all over eat her pussy until she's dripping..would be nice if I could alternate eating you as well. Will she get off watching us?"
	"Thoughts and I have more…"

21. On October 22, 2019, the OCE and Joe Smo planned to meet on October 24, 2019 in Henrico County, Virginia, at 3pm. Joe Smo stated he would be driving a 2019 Hyundai Elantra.

22. On October 23, 2019, the OCE and Joe Smo had the following exchange:

Joe Smo:	"I'm forcing myself not play with myself..i usually do daily sometimes twice…lol"

OCE:	"Sorry had to get the girls in the bus"
	"Twice a day?? Lol damn"
Joe Smo:	"Yes I told you I'm always horny"
	"That energy will go to you and Krys now..."

23. During the totality of the chats, Joe Smo sent the OCE numerous pictures of himself, including one stating he just got his first tattoo on September 7, 2019. One image is that of him sitting at what appears to be a tattoo parlor with his left arm raised exposing a tattoo on his left inner forearm. The tattoo is of a scorpion.

B. Identification of the Subject

24. A search of publicly available data bases for cell phone number 703-401-XXXX, the same number referenced in paragraph 42, reveals the telephone number belongs to LOUIE FERNANDO LEITAO, date of birth November 4, 19XX.

25. A query of the Department of Motor Vehicles (DMV) database revealed that LOUIE FERNANDO LEITAO holds a Virginia Driver's License, with an address of record as the PREMISES, and a registered 2019 Hyundai 4 door sedan with license plate UPW-3801. The picture on his DMV record also matched the pictures on Joe Smo's Alt.com profile and the picture he sent during the chat sessions.

26. On September 30, 2019, investigators received subscriber data from Kik for user ID "Joe Smo" "Carika2016." The results revealed the account was registered on July 31, 2017, and the email associated with the account was "joesmo@coxnet." The Kik registration email

matched the email address provided to the OCE by "Joe Smo" in an electronic message on Alt.com on July 29, 2019.

C. Criminal Complaint and Arrest

27. On October 23, 2019, the Hon. Roderick C. Young, United States Magistrate Judge, signed a Criminal Complaint charging LOUIE FERNANDO LEITAO with Coercion and Enticement, in violation of 18 U.S.C. § 2422(b). The Court also authorized a search warrant for LEITAO's Hyundai sedan.

28. On October 24, 2019, LOUIE FERNANDO LEITAO did, in fact, appear at the previously agreed-upon location in Henrico County, Virginia, to meet the OCE. He was driving the 2019 Hyundai 4 door sedan with the license plate UPW-3801. Law enforcement arrested LEITAO when he arrived on the Criminal Complaint.

D. Connection to the PREMISES

29. Law enforcement gave LEITAO his *Miranda* warnings and he agreed to voluntarily speak with law enforcement. During his interview, LEITAO said that he saved child pornography images on a laptop and thumb drive at the PREMISES. LEITAO said that he resided at the PREMISES with his wife, who is out of the country until October 30, 2019. LEITAO also told law enforcement that his adult daughter, who lives within the Eastern District of Virginia, has a key to the house.

30. On October 25, 2019, law enforcement executed a duly-authorized search warrant on the cell phone in LEITAO's possession at the time of his arrest. Law enforcement preliminarily observed child pornography images on the phone.

E. Child Pornography Collectors

31. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors").

32. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

33. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

34. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

35. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

TECHNICAL TERMS

36. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service

providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

38. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

39. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

40. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

42. Because LEITAO shares the PREMISES with his wife, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

43. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

John P. Houlberg
Special Deputy United States Marshal
FBI Child Exploitation Task Force
Federal Bureau of Investigation

Subscribed and sworn to before me on October 28, 2019.

/s/
Ivan D. Davis
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched is 9923 Stone Wood Court, Burke, VA, 22015, further described as a split-level style single dwelling house. The house consists of a combination of brick and gray vinyl siding, with black shutters. There is a concrete driveway is at the right edge of the property which leads to an attached garage with a single garage door. Above the garage in black script are the letters written out "Ninety-Nine Twenty-Three". There is a sidewalk leading from the driveway to the front door of the residence, which is situated approximately in the center of the front of the residence. The front door appears to be a solid 4 panel door with a small glass window on the top of it, and has a glass storm door attached to it. On the left side of the residence is another entry door. This door appears to be a white door with glass windows on the top half of it.

ATTACHMENT B

Property to be seized

1. All records and information relating to possible violations of the following criminal offenses: distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252A; and online enticement, in violation of 18 U.S.C. § 2422(b), including:

   a. Any and all visual depictions of minors;

   b. Any and all communications with minors;

   c. Any and all address books, names, and lists of names and addresses of minors;

   d. Any and all diaries, notebooks, notes, and any other records reflecting physical contact, whether real or imagined, with minors, and any such items discussing sexual activities with minors;

   e. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;

   f. Records and information relating to Alt.com and/or Kik username/account jmsoqueenIVY, Joe Smo, Carika2016, and any related Alt.com or Kik accounts;

   g. Records and information relating to the email accounts "joesmo@coxnet" and any related email accounts;

   h. Any information recording suspect's schedule or travel from October 23, 2019 to October 24, 2019.

2. Computers or storage media (hereinafter, "COMPUTER") used as a means to commit the violations described above.

3. For any COMPUTER whose seizure is otherwise authorized by this warrant, and any COMPUTER that contains or in which is stored records or information that is otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect the COMPUTERS to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smart phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

* * *

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.